REMARKS

Claims 1-7 and 9-21 are pending in this application. Reconsideration and allowance in view of the following remarks are respectfully requested.

I. THE CLAIMS DEFINE PATENTABLE SUBJECT MATTER

A. The Rejection of Claims 1-4, 6, 7, 9-15, 17 and 19-21

In paragraph 3, the pending Office Action rejects claims 1-4, 6, 7, 9-15, 17 and 19-21 under 35 U.S.C. 103 by Freund, U.S. Patent No. 5,987,611 in view of He, U.S. Pat. No. 6,088,451. This rejection is respectfully traversed.

Claim 1 recites a method for providing accessibility to a plurality of remote service providers across a network via a single login to a host service provider, each of the plurality of remote service providers being accessible through the host service provider and each of the plurality of remote service providers having separate login procedures requiring data, the method comprising the steps of the host service provider receiving the single login from a user, the host service provider having a universal session manager; the universal session manager retrieving data from a validation database based on the single login to the host service provider, wherein the data is effective for accessing a selected one of the plurality of remote service providers, and wherein the data is based at least in part on the single login; the universal session manager transmitting said data to the remote service provider, the universal session manager and the remote service provider exchanging the data to effect a two-sided authentication; and the host service provider directing the user to the remote service provider.

The Examiner is respectfully requested to reconsider and withdraw the rejection as set forth in the Office Action. As reflected in claim 1, the teachings of Freund are substantially different then the present invention, and as discussed below, He fails to cure the deficiencies of Freund.

In paragraph 3, the Office Action alleges various assertions as to the manner in which Freund teaches the claimed invention. The Office Action asserts that as to claim 1, Freund discloses a method for accessing one of a plurality of remote service providers (web server 350's of fig. 3B can be Internet Service providers) across a network via a single login to a host service provider (320a fig. 3B), each of the plurality of remote service providers being accessible through the host service provider, and each of the plurality service providers having separate login procedures requiring data.

The Office Action further asserts that Freund teaches the host service provider (320a fig. 3B) receiving the single login (providing remote login from clients 31 O's fig. 3A), the host service provider (see abstract, fig. 3B, col. 21 line 47 to col. 22 line 21). The Office Action asserts that Freund teaches a universal session manager (373 fig. 3B) retrieving data from a validation database (374 fig. 3B) based on the single login, wherein the data is effective for accessing a remote service provider and is based at least in part on the received username and password (i.e., monitoring user access, col. 22 line 23 to col. 23 line 55). These assertions as set forth in the Office Action are respectfully traversed.

For the reasons set forth herein, Freund and/or He fail to teach or suggest the invention as recited in claim 1. Freund is directed to a system and methodology for managing internet access on a per application basis for client computers connected to the internet. Applicant respectfully submits that this title is representative, and that Freund relates to Internet access - and is different than the claimed invention.

The features of claim 1 are noted above. Applicant submits that Freund, in particular, fails to teach the claimed interrelationship between the universal session manager, the host service provider and the remote service provider, as recited in claim 1, and that He fails to cure the deficiencies of Freund..

In column 8, lines 40-65, Freund describes an Internet access monitoring system including that: (1) the system should preferably be capable of restricting access to the Internet (or other Wide Area Network) to certain approved applications or/and application versions. (2) The system should preferably support centrally-maintained access rules (e.g., defining basic access rights), but at the same time allow individual workgroup managers or even individual users to set rules for their area of responsibility, if so desired by the organization. (3) The system should preferably prevent users from circumventing Internet access rules, either accidentally or intentionally. Freund describes that it should be difficult, for instance, for a user to circumvent access rules by connecting to the Internet through a dial-up connection (e.g., connecting to an ISP with a modem). Similarly, it should be difficult for a user to circumvent access rules by uninstalling or tampering with components of the system, from his/her own PC.

Freund teaches further aspects relating to Internet access in column 10, lines 55-65. Freund teaches that the ability to monitor and regulate Internet access on a per application basis is particularly advantageous. Advantages include, for instance, the ability to specify which applications can (and cannot) access the Internet. Freund describes that IS departments have a strong interest in limiting the number of applications used on their LANs, including limiting available applications to a uniform set of "approved" applications. For one, user support is simplified if fewer different applications are in use. Further, Freund teaches, the overall integrity of one's corporate networks is improved if known applications (or unknown versions of applications) are used.

In the rejection, the Office Action refers to the teachings of Freund in columns 21 and 22. In column 22, lines 7-21, for example, Freund teaches that in an embodiment of Freund, the ISP installs an additional central server component 370 to host the central supervisor application; this new component comprises an ISP authentication server 371 and an ISP supervisor server 372 (which includes a central supervisor application 373). After the central ISP authentication server 371 has established the authenticity of the user, it contacts the central supervisor application 373 in order to find out if the user has established additional access monitoring services. In such a case, the ISP authentication server 371 signals the POP server 320a to only allow limited access to the Internet and redirect all requests to a "Sandbox" server application, shown at 374, on the central supervisor server 372. This "Sandbox" server 374 restricts the client's Internet access to a very limited account maintenance site. Aspects of the sandbox server 374 vis-à-vis the rejection are discussed further below.

In conjunction with the other features, claim 1 of the present invention recites the host service provider having a universal session manager, the universal session manager retrieving data from a validation database based on the single login to the host service provider, wherein the data is effective for accessing a selected one of the plurality of remote service providers, and wherein the data is based at least in part on the single login. Of particular note vis-à-vis the teachings of Freund, claim 1 recites the universal session manager transmitting said data to the remote service provider, the universal session manager and the remote service provider exchanging the data to effect a two-sided authentication; and the host service provider directing the user to the remote service provider.

Thus, claim 1 recites a particular interrelationship between the universal session manager and the remote service provider. Freund fails to teach this interrelationship.

The Office Action attempts to cure the deficiencies of Freund with the teachings of He. That is, the Office Action acknowledges that Freund does not disclose transmitting data to the remote service provider and directing the user to the remote service provider after the remote service provider exchanging the data to effect a two-sided authentication and the host service provider directing the user to the remote service provider. The Office Action asserts that however, He discloses transmitting data to the remote service provider and directing the user to the remote service provider after the remote service provider exchanging the data to effect a two-sided authentication and the host service provider (credential server 204 fig. 2) for directing the user to the remote service provider (using credential server 204 to manage user credentials with authentication server 202, see fig. 2, abstract, see col. 11 line 54 to col. 12 line 33 and col. 12 line 65 to col. 13, line 63).

The Office Action proposes to combine the teachings of Freund and He. Specifically, the Office Action asserts that it would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement He's teachings into the computer system of Freund to control network access because it would have relieved the administrative burden to effectively and efficiently control and manage user credentials and thus enabled the enhanced the effectiveness of the access control mechanisms. These assertions as set forth in the Office Action are respectfully traversed for various reasons as set forth below.

Applicant respectfully submits that the rejection is fully unclear as to the manner in which the applied art is being combined. On page 3, line 3, the Office Action asserts that Freund discloses a method for accessing one of a plurality of remote service providers (web server 350's of fig. 3B can be Internet Service providers) across a network via a single login to a *host service provider (320a fig. 3B)*, each of the plurality of remote service providers being accessible through the host service provider. Such assertion clearly reflects that the Office Action is interpreting Freund's component 320a, i.e., a POP server, as the claimed "host service provider." In contrast to such assertion, on page 3, third to last line, the Office Action asserts that He discloses a *host service provider (credential server 204 fig. 2)* for directing the user to the remote service provider. It is thus fully unclear what the Office Action is interpreting to allegedly constitute the claimed host service provider. Further, it is unclear the manner in which the Office Action proposes to modify Freund based on He, so as to allegedly teach the claimed invention. Clarification of the rejection is requested.

As noted above, the Office Action asserts that He discloses transmitting data to the remote service provider and directing the user to the remote service provider after the remote service provider exchanging the data to effect a two-sided authentication and the host service provider (credential server 204 fig. 2) for directing the user to the remote service provider. Applicant respectfully submits that such assertions fail to reflect the features of claim 1 vis-à-vis the teachings of He.

Claim 1 recites the universal session manager retrieving data from a validation database based on the single login to the host service provider, wherein the data is effective for accessing a selected one of the plurality of remote service providers, and wherein the data is based at least in part on the single login; the universal session manager transmitting said data to the remote service provider, the universal session manager and the remote service provider exchanging the data to effect a two-sided authentication; and the host service provider directing the user to the remote service provider. Accordingly, claim 1 recites a particular interrelationship between the universal session manager and the remote service provider. He fails to teach this relationship.

He is directed to a security system and method for network element access. In column 2 lines 12-24, He teaches the security system provides security mechanisms using a network security server coupled to a network. The network security mechanisms include an authentication server, a credential server, and a network element access server. The method controls access to network elements by user elements and protects network resources and information. The method provides authentication of the network users to the network elements using the authentication server. Managing network user credentials or privileges is performed by the credential server, associated with the authentication server. Access to the network elements by the user elements is controlled by the network element access server, associated with the authentication server and the credential server.

Of particular note, He teaches that in the processing, a general *ticket* is provided to each user element at log on to facilitate future access requests. The general ticket is presented to the network security server each time the user element initiates a communication session. The general ticket is used by the network security server to authenticate access requests without having to verify user credentials for each access request. If upon initiation of a communication session the general ticket is authenticated, the network security server generates a *session ticket* and provides the user element with the session ticket and a unique session encryption key. The session ticket is used by the user element to communicate with the selected network element. Applicant submits that the utilization of He's ticket, as discussed further below, is different than the interrelationship set forth in the claimed invention.

The Office Action references columns 11-13 of He, and asserts that He's credential server 204 teaches the claimed host service provider. In column 11, lines 34-40, He teaches that three components in FIG. 2 for providing network security solutions include a network authentication 202, user credential control 204 and network element access control 206. Collectively, these three components are generally referred to as a network security server (NSS; also called the master server), as shown at dashed box 208 of He.

He describes processing of the network authentication 202, user credential control 204 and network element access control 206 in column 18, line 42 - column 19, line 31. He teaches that user credential/privilege control is centrally controlled by the credential server 204. Through message exchanges with the credential server 204 with the correct *ticket*, a user will obtain the list of certified credentials that the network elements 104 can rely on to make further access decisions that are reached based on the user credentials. The basic requirement for the message exchanges is to have necessary functional modules in the credential server 204 and in the user element 102 through which the user performs the required steps to get the list of certified credentials. The key for the user to achieve this credential certification is that the user possess the correct ticket issued by the authentication server 202 at the time of network authentication.

He teaches the user sends a message to the credential server 204 to request for a list of the user credentials. The message contains the ticket obtained by the user from the authentication server 202. The credential server 204 will not accept and process the request without being presented with the correct ticket from the user.

Further, at column 18, line 66, He teaches upon receiving the request message, the credential server 204 retrieves the information in the ticket and verifies that the request is indeed sent from the correct user. Based on the user identifier, the credential server 204 will retrieve the list of user credentials from the registration database 210 and enclose the list in a credential ticket. The credential ticket is sent back in a response message and will be used for the user to communicate with the network element access server 206. This utilization of tickets is different than the claimed invention.

He discusses processing of the network element access server 206 in column 13, lines 43-63, referenced in the Office Action. In particular, He teaches to gain the right to access a network element, the user communicates with the network element access server 206 to specify the name of the network element 104. Upon receiving the access request, the network element access server 206 will check an internal access matrix to determine whether the user is allowed any access at all to the specified network element 104.

Of particular note, He teaches if such check is successful, the network element access server will *issue a certificate or ticket to the user*. The ticket is the necessary piece of information that has to be presented in all communication between the user and the network element 104 for access to any resources and information in the element.

In contrast to He's manipulation of the *certificate or ticket to the user*, claim 1 recites the universal session manager transmitting said data to the remote service provider, the universal session manager and the remote service provider exchanging the data to effect a two-sided authentication. He fails to teach such processing. Instead, He teaches the use of tickets, as described above.

As noted above, the Office Action asserts that it would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement He's teachings into the computer system of Freund to control network access because it would have relieved the *administrative burden to effectively and efficiently control and manage user credentials* and thus enabled the enhanced the effectiveness of the access control mechanisms. As discussed above, Applicant submits that the Office Action is fully unclear as to the manner in which the Office Action proposes to modify Freund based on the teachings of He.

Applicant further submits that the one of ordinary skill would not have been motivated to combine the teachings of Freund and He as proposed in the Office Action. The very basis of the motivation to combine He's teachings into Freund is to control network access. See Office Action page 4, line 3. However, the title of Freund's invention is system and methodology for managing internet access on a per application basis for client computers connected to the internet. That is, Freund itself is directed to control network access. Accordingly, Applicant submits that the motivation for combination as set forth in the Office Action is simply not supportable, i.e., in that the motivation is based on an alleged deficiency of Freund, which is simply not present.

Applicant respectfully submits that Freund and He fail to teach or suggest the features of claim 1 for at least the reasons set forth above. Further, claim 7 is allowable at least for some of the reasons discussed above with respect to claim 1. Further, the various dependent claims recite patentable subject matter at least for their various dependencies on claims 1 and 7, as well as for the additional subject matter recited in such dependent claims.

B. The Rejection of Claims 5, 16 and 18 under 35 U.S.C. §103

In the Office Action, claims 5, 16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freund and He and in view of Kirsch U.S. Patent No. 5,963,915.

The Office Action asserts that Freund does not specifically disclose a triple handshake and a cookie, but that however, Kirsch discloses a triple handshake and a cookie (i.e., providing a cookie and a series of handshake transactions to negotiate the establishment of the secure transactions between the servers, see col. 2 lines 1-46 and col. 8 lines 12-63). The Office Action further alleges that it would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement Kirsch's teachings into the computer system of Freund to process data transaction over the Internet because it would have provided automatic simultaneous purchase transactions handling for both secure and insecure client browsers and increased levels of authentication of data communications in the Internet.

Illustratively, Kirsch teaches in column 4, lines 48-64, that the Kirsch invention provides for a purchase transaction that appears to the client user as a singular selection of a purchasable product or service and a singular confirmation of the purchase. A persistent predetermined coded identifier is established on the client browser corresponding to an account record stored by the merchant server. Kirsch further teaches that a predetermined URL referencing a purchasable product or service is served to the client browser.

Further, Kirsch teaches that a facility known as persistent client-side cookies has been introduced to provide a way for server systems to store selected information on client systems. Cookies are created at the discretion of the server system in response to specific client URL requests. Part of the server response is a cookie consisting of a particularly formatted string of text including a cookie identifier, a cookie path, a server domain name and, optionally, an expiration date, and a secure marker. Kirsch further describes that a conventional uniform resource locator (URL), utilizing "https" as the secure HTTP protocol identifier, is issued by the client browser to specifically request a secure client/server session. A series of handshake transactions are provided to negotiate the establishment of the secure session including performing an encryption key exchange that is used in an encryption algorithm implemented by both the client-side and server-side secure sockets layers.

However, Applicant submits that even if it were obvious to somehow use Kirsch's teachings relating to cookies and authorization techniques, which Applicant does not admit to be the case, to modify Freund, such combination would still fail to teach or suggest the claimed invention.

It is submitted that Freund, He and Kirsch, either alone or in combination, fail to teach or suggest the claimed invention. Withdrawal of the 35 U.S.C. §103 rejection is respectfully requested.

II. CONCLUSION

For at least the reasons outlined above, Applicant respectfully asserts that the application is in condition for allowance. Favorable reconsideration and allowance of the claims are respectfully solicited.

For any fees due in connection with filing this Response the Commissioner is hereby authorized to charge the undersigned's Deposit Account No. 50-0206.

Should the Examiner believe anything further is desirable in order to place the application in even better condition for allowance, the Examiner is invited to contact Applicant's undersigned representative at the telephone number listed below.

Respectfully submitted,
HUNTON & WILLIAMS

James R. Miner
Registration No. 40,444

Hunton & Williams
1900 K Street, N.W., Suite 1200
Washington, D.C. 20006-1109
(202) 955-1500

Dated: October 5, 2005